



## INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification <sup>6</sup> : <b>G06F 1/00, G09B 7/02</b>		<b>A1</b>	(11) International Publication Number: <b>WO 99/36848</b>
			(43) International Publication Date: 22 July 1999 (22.07.99)
(21) International Application Number: PCT/US99/00481		(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).	
(22) International Filing Date: 8 January 1999 (08.01.99)			
(30) Priority Data: 60/071,926 20 January 1998 (20.01.98) US			
(71) Applicant (for all designated States except US): EXAMSOFT WORLDWIDE, INC. [US/US]; Suite B, 1020 Northwest 6th Street, Deerfield Beach, FL 33442 (US).			
(71)(72) Applicants and Inventors: STORAGE, William, K. [-/US]; Apartment 1-103, 2 Townsend Street, San Francisco, CA 94107 (US). WASSERMAN, Adam, M. [-/US]; Apartment 2-205, 2 Townsend Street, San Francisco, CA 94107 (US).			
(74) Agents: TACHNER, Adam, H. et al.; Crosby, Heafey, Roach & May, Suite 1900, 4 Embarcadero Center, San Francisco, CA 94111-4106 (US).			

## Published

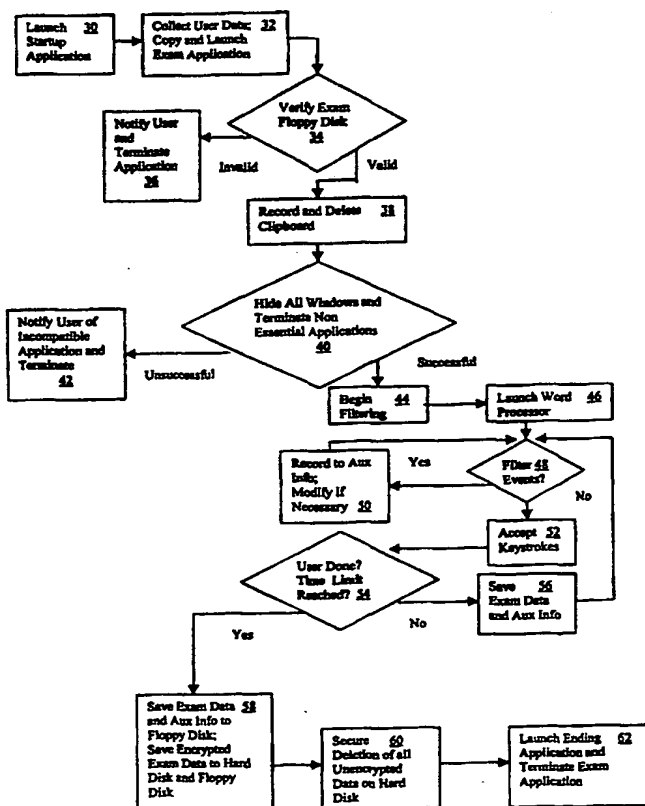
With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

## (54) Title: SECURE EXAM METHOD

## (57) Abstract

A method and computer program are provided for creating a secure computing environment by preventing access to unauthorized files during the execution of a desired application. User commands are filtered for instructions that would lead to unauthorized application access. This restricts access to all files except the file created by the desired application. This method works for portable, desktop, and networked computers. Preferably, at least the security features of the invention are distributed to the users through a single-use floppy disk, although any other suitable storage medium may be utilized. Additional security features include the use of encrypted files, a log of system events and the secure deletion of related files.



**FOR THE PURPOSES OF INFORMATION ONLY**

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

## SECURE EXAM METHOD

### RELATED APPLICATIONS

This application depends for priority upon U.S. Provisional Patent Application Ser. No. 60/071,926, filed on January 20, 1998 and entitled COMPUTER HARD DRIVE LOCK OUT DEVICE FOR GIVING SECURE EXAMS.

### FIELD OF THE INVENTION

The present invention relates generally to the field of computer security and more particularly to computer software for restricting access to a computer's stored data and applications for the purpose of giving secure exams.

### BACKGROUND OF THE INVENTION

Portable and desktop computers equipped with word processing software have become the primary tool for preparing written material. One area where the use of all types of computers has lagged, however, is in the field of test taking. Despite the desire of students to write essay exams with the aid of a computer, concerns about security have severely curtailed their use. In the prior art, computer use in test taking environments have typically required the use of dedicated computers to ensure that unauthorized data or programs are not present. Needless to say, supplying a dedicated computer to each student desiring one when taking a test represents a significant if not insurmountable expense.

1           Accordingly, what has been needed is a method to allow the use of a personal  
2 computer to prepare answers to an exam while preventing access to unauthorized programs  
3 and data that might be stored in the computer. This invention satisfies these and other needs.  
4

#### 5           **SUMMARY OF THE INVENTION**

6           The present invention comprises a method and system for preventing access to data  
7 and programs stored by a computer while allowing the computer to execute a desired  
8 application, comprising the steps of, and executable instructions for, closing unauthorized  
9 programs, filtering user commands to prevent unauthorized access to files stored on the  
10 computer, and allowing filtered user input to the desired application. Normally, the filtered  
11 user input is periodically saved and updated. Preferably, the application for the closing and  
12 filtering steps resides on a floppy disk to enhance the security of the system, although  
13 alternative embodiments allow for execution independent of floppy disks. Native features of  
14 the computer's operating system are accessed to filter, and if necessary, modify, commands  
15 entered by the user to create a secure computing environment. Accordingly, the only file that  
16 is active and accessible is the one created by the user in response to the desired application. A  
17 number of additional security measures may be implemented, including encrypting files,  
18 recording system events and securely deleting files. In preferred embodiments, the invention is  
19 used to administer an examination.  
20

#### 21           **BRIEF DESCRIPTION OF THE DRAWINGS**

22           The aforementioned advantages of the present invention as well as additional  
23 advantages thereof will be more clearly understood hereinafter as a result of a detailed  
24 description of a preferred embodiment of the invention when taken in conjunction with the  
25 following drawings.

1           FIG. 1 is a schematic representation of a computer system useful in the practice of the  
2 present invention.

3  
4           FIG. 2 is a flowchart showing the primary steps in the methods of the present  
5 invention.

### 6 7           DETAILED DESCRIPTION OF THE DRAWINGS

8           As shown Fig. 1, a typical computer system useful in the practice of this invention  
9 generally comprises a central processing unit (CPU) 10, having volatile and nonvolatile  
10 memory 12 as well as recordable storage such as a hard drive 14 and a floppy disk drive 16.  
11 Conventionally, the user input devices include a keyboard 18 and a pointing device, such as a  
12 mouse 20. Other input devices may also be used including a graphics tablet or a microphone  
13 in conjunction with voice recognition software. The computer system also comprises a display  
14 22 and, optionally, other output devices such as speakers, printers and the like. CPU 10 may  
15 also be connected to a network (not shown).

16  
17           In preferred embodiments, the invention has been designed to eliminate academic  
18 dishonesty by taking control of an operating system through execution of a software program  
19 that locks out access to applications, macros, files, programmed key commands and  
20 networked files stored in computer-readable media. Generally, any file, application or data,  
21 that could be used to gain an unfair advantage in taking an exam should be considered  
22 unauthorized and access to that file should be restricted. As used herein, computer-readable  
23 media refers to any storage device for computer-readable data, including non-volatile memory  
24 such as hard disk drives, floppy disk drives, ROM, writable or read-only CD-ROMs, DVD  
25 drives, tape drives, PC cards and the like and volatile memory such as RAM. The materials

1     secured by this invention may also be stored in computer-readable media available over a LAN  
2     or WAN, accessible via a modem, an Ethernet link, or any other network connection. Access  
3     to all of these sources of data and applications is completely restricted. The exam answer is  
4     preferably recorded to a specially created exam file using the exam application's own easy to  
5     use word processor.

6  
7             The present invention capitalizes on the fact that most modern operating systems  
8     prevent programs from directly interacting with peripherals such as the display, keyboard and  
9     mouse by providing interfaces for such services. Programs therefore communicate indirectly  
10    with the screen, keyboard, and mouse through these defined interfaces using information  
11    packages known as messages. The invention filters these messages to prevent the user from  
12    accessing unauthorized data or programs. In a preferred embodiment, the invention employs a  
13    compiled 16 or 32-bit executable file designed for the Microsoft Windows 3.x, Windows 9x or  
14    Windows NT (all of which are federally registered and recognized trademarks of Microsoft,  
15    Inc.) operating system that uses a number of supporting executable files in dynamic link  
16    libraries. The system may also be adapted for use with other operating systems as necessary,  
17    as understood by one skilled in the art to which the present invention pertains. In these  
18    embodiments, the invention uses native services of the operating systems to achieve a message  
19    interception scheme referred to herein as cross-processing subclassing.

20  
21            Subclassing is the process of intercepting operating system messages that are normally  
22    processed behind the scenes. The Windows environment sends messages indicating that  
23    system events have occurred, such as keyboard input or mouse selection. Windows also sends  
24    housekeeping messages to control the display of each window. Subclassing intercepts each of  
25    these messages, allowing them to be modified or deleted before passing them on to their

1 intended destination. In part, Windows achieves subclassing through the use of hooks to be  
2 monitored, intercepted, and discarded by a program.

3  
4 In the Windows operating system, a hook is a mechanism by which a function can  
5 intercept events such as messages, mouse actions, and keystrokes before they reach an  
6 application or even the main body of the operating system, which otherwise would direct these  
7 to the application currently in use. This mechanism is provided as a "service" by the operating  
8 system. Hooks are provided by calling the appropriate set of functions residing in the  
9 operating system and by supplying filter functions to the operating system. Specifically, the  
10 operating system will automatically call the programmer supplied filter function when the  
11 hooked event occurs.

12  
13 The filter function can act on events and, in some cases, modify or discard them. For  
14 example, a filter function might want to receive all keyboard or mouse events. For Windows  
15 to call a filter function, the filter function must be installed—that is, attached—to a Windows  
16 hook (for example, to a keyboard hook). Attaching one or more filter functions to a hook is  
17 known as setting a hook. If a hook has more than one filter function attached, Windows  
18 maintains a chain of filter functions. The most recently installed function is at the beginning of  
19 the chain, and the least recently installed function is at the end.

20  
21 The invention enlists these services to monitor messages concerned with keystrokes,  
22 the Windows clipboard, the creation of windows, the creation of other programmatic  
23 processes, and the visibility of windows. The invention intercepts, discards, and preferably  
24 makes a record of all messages that could allow the user to start another program or access an  
25 unauthorized file in any way. Although this monitoring activity requires a significant portion

1 of the systems resources, the vast majority of portable computers with 80386 or better  
2 processors can quickly execute it. One having ordinary skill in the art can modify the  
3 invention as necessary to adapt it to other operating systems.  
4

5 In a preferred embodiment, users install most of the program's files through an  
6 installation kit. Users run an automated installer program to place required files on their hard  
7 drives. Normally, installation will be done before exam day, but since the procedure takes  
8 only a few minutes, it may be performed immediately prior to an exam, if necessary. Any  
9 installation disks preferably contain supporting files only, not the actual application, so no  
10 security issue is raised by an early installation. A demonstration version of the program may  
11 be included in the installation kit to allow the user to become familiarized with the program,  
12 and in particular, with the word processing features of the application. In preferred  
13 embodiments, the security features of the invention are not included in the demonstration  
14 version.  
15

16 Immediately prior to the test, a sealed single-use exam disk is distributed to each user  
17 much the way an exam bluebook would. Currently, floppy disks are widely used as a  
18 removable computer-readable media but as the demand for increased storage grows, other  
19 types of removable media may predominate, such as ZIP and JAZ disks available from  
20 IOMEGA, Inc. , the LS-120 Supper Floppy Disk, writable CD-ROMs and DVDs and the like.  
21 The invention can be adapted to work with any removable computer-readable media. The  
22 exam disk contains the security features of the invention as well as password and creation date  
23 verification data. In preferred embodiments, as discussed below, the exam application is  
24 temporarily copied to the user's hard disk to improve performance. In these embodiments, the  
25 starting and ending sub-applications of the present invention perform the necessary copying,



1 execution and deletion of the exam application. In other embodiments, it may be desirable to  
2 execute the exam application from the floppy disk directly. In such embodiments, the starting  
3 and ending sub-applications are unnecessary.

4  
5 Fig. 2 shows a flowchart that represents major steps of the invention. First, the user  
6 inserts the exam floppy disk and launches the startup application at step 30. The startup  
7 application prompts the user for personal data, and then records it to the floppy disk at step  
8 32. The startup application also preferably temporarily copies the exam application from the  
9 floppy to the user's hard drive to improve performance. The exam application can be run  
10 from the floppy disk, but generally it is preferable to use the hard disk drive to decrease seek  
11 times and improve data transfer rates. This preferable embodiment may also be adapted to use  
12 with computer networks in a manner independent of removable media. The startup program  
13 then launches the exam application and terminates itself. The exam application creates an  
14 auxiliary information file on the user's hard drive and on the floppy disk to record a log of the  
15 application's execution. Then, the exam application verifies that the floppy disk is valid by  
16 password and creation date at step 34. If the floppy disk is not valid, the application notifies  
17 the user and terminates if necessary at step 36.

18  
19 After determining the floppy disk is valid, the exam application implements the security  
20 features of the invention. The exam application records the contents of the clipboard to the  
21 auxiliary information file on the hard disk and then deletes the clipboard at step 38. The exam  
22 application identifies already running processes by sequentially obtaining a thread for each  
23 process and then a process ID for each thread. A process is a logical grouping of a memory  
24 address space (memory area allocated by the operating system), a computer program, and its  
25 data. Normally, there is no interaction between programs in different processes, and they

1 cannot read or write to memory space outside their process, without prior agreement by both  
2 programs, such as object linking and embedding (OLE). Each process consists of one or more  
3 threads of execution. These threads are simply atomic units of code execution that can run  
4 simultaneously within a single process.

5  
6 While some processes are essential to the functioning of the operating system, many  
7 others are not and may pose a security concern. Essential processes are those that are  
8 necessary for the stable operation of the operating system and for the execution of the exam  
9 application. In general, all nonessential processes are considered unauthorized and are closed  
10 or otherwise hidden. The exam application sends a SC\_CLOSE message to the window of  
11 each running process that is not essential to Windows functions or otherwise terminates those  
12 programs at step 40. If the exam application encounters processes that cannot be closed it  
13 either hides its windows or notifies the user of the conflict and quits at step 42. Similarly,  
14 some applications such as crash protection programs interfere with the subclassing functions  
15 of the exam application. If the exam application identifies such incompatible programs, it  
16 notifies the user and/or quits.

17  
18 After controlling the running processes, the exam application then configures Windows  
19 for optimum security. Specifically, the exam application terminates or hides the Explorer  
20 windows in Win9x and NT systems, depending on type. The application also turns off screen  
21 savers, power management, the desktop wall paper, sets the desktop icons invisible and then  
22 updates the .INI files to reflect the changes. Next, the exam application disables the task bar  
23 in Win9x and NT versions. Finally, the exam application identifies itself to the operating  
24 system as an active screen saver to prevent the Ctl-Alt-Del keystroke combination in Win9x.

1           After terminating non essential processes and securing the operating system  
2 configuration, the exam application sets the appropriate hooks and begins cross-process  
3 subclassing at step 44. Specific steps taken depend on the variety of Windows, but generally  
4 include:

- 5           · Setting a hook for Ctl-Esc keys in Win 9x
- 6           · Setting a hotkey message hook (WM\_HOTKEY) to intercept but not block Ctl-Esc
- 7           in Win NT
- 8           · Setting a hook for the foreground window to reset it to the exam application in Win
- 9           NT
- 10          · Setting a hook for clipboard usage to block paste commands where source is not the
- 11          exam application
- 12          · Setting a hook and subclassing for window creation (the WM\_CREATE message)

13  
14          Having secured the computer's operating system, the exam application can begin the  
15 examination by showing a word processor window at step 46. The program can easily be  
16 adapted to other types of examination such as multiple choice or short answer by substituting  
17 the appropriate form for the word processing window.

18  
19          The exam application monitors all the keystrokes and other user input as the  
20 examination proceeds at step 48. The exam application records the details of all intercepted  
21 hooked messages, such as attempts to call unauthorized applications at step 50 or access  
22 unauthorized data. While a few attempts to call unauthorized applications or data may occur  
23 inadvertently, more frequent occurrences may indicate an attempt to subvert the security

1 features of the exam application and will be reviewable by the exam grader. Keystrokes and  
2 other user input that pass the filter function are passed on to the word processor at step 52.

3  
4 The exam application periodically performs several monitoring functions. First, the  
5 examination application checks the visible windows to confirm that the only active windows  
6 are related to the examination. This offers a level of redundant protection over the filtering of  
7 the WM\_CREATE message. The exam application also periodically saves the status of the  
8 exam and performs several updates at step 54, preferably once a minute. The exam data and a  
9 backup are saved to disk, as well as test taking statistics such as the number of keystrokes and  
10 total number of characters added to the data file per monitoring interval at step 56. These  
11 statistics are added to the auxiliary information file and can be used to resolve questions about  
12 exam security. For example, delays between the periodic saves indicates that the exam  
13 application was not active. If the delay is longer than that required to restart the exam  
14 application with a proctor disk (discussed below), it may be an indication that the user was  
15 attempting to subvert the program. Also, the number of keystrokes can be compared to the  
16 total number of characters added. Large discrepancies may indicate that text was copied from  
17 another source. Yet other features such as a clock display and word count can also be  
18 periodically updated. Towards the end of the allotted time, a reminder, audible or visible, can  
19 alert the user.

20  
21 At the conclusion of the exam, the program saves a Rich Text Format (RTF), or  
22 otherwise suitably formatted document to the floppy disk in the computer's floppy disk drive  
23 and saves encrypted copies to both the floppy disk and the hard disk at step 58. A copy of the  
24 auxiliary information file is also saved to the floppy disk. Further, the user may be given the  
25 option to save an additional encrypted copy of the exam data for backup purposes. In the

1 event of a dispute regarding the contents of the floppy disk or if the floppy disk becomes  
2 erased or lost, the encrypted copy or copies on the hard drive provide a secure record of the  
3 exam. After the various files are saved to the floppy and hard disks, each unencrypted file on  
4 the hard drive is securely deleted by overwriting several times the hard drive sectors where the  
5 data was stored at step 60. Finally, the exam application launches the ending application,  
6 restores the computer's settings and then terminates itself at step 62. The ending application  
7 securely deletes the temporary copy of the exam application from the hard disk and terminates  
8 itself. In some embodiments, it may be desirable to have the ending application shut down the  
9 computer.

10  
11 To accommodate system crashes or loss of power, attempts to restart the exam  
12 application must be approved by a proctor. After restart, the starting application prompts the  
13 user for personal information as in the normal sequence. However, the floppy disk does not  
14 pass the password and creation date verification as it is allowed only one execution.  
15 Accordingly, the exam application terminates, requiring and preferably visually requesting a  
16 valid proctor disk. If the proctor determines that a restart is warranted, the proctor will supply  
17 a proctor floppy disk. As with the exam disks, any computer-readable removable media may  
18 be used as a proctor disk. Verification of a valid proctor disk allows the exam application to  
19 restart and the user can replace the floppy disk and commence work from the last saved  
20 version. In other embodiments, it may be desirable to replace the proctor disk with a  
21 hardware component that could plug into a parallel port, a serial port, a PC Card slot or the  
22 like. Once the exam application identifies the appropriate hardware, it restarts the exam from  
23 the last saved version.

1           As discussed above, the exam application is tailored to the type of examination being  
2 given. In most applications, it will be desirable to provide word processing functions to  
3 facilitate responses to essay questions. Preferably, the word processing program is configured  
4 to operate similarly to popular commercial word processing programs. The exam application  
5 can automatically add headers and footers having the users name or ID number, course  
6 instructor and other course information to aid identification. The exam application can easily  
7 be modified to allow its use for multiple choice or short answer questions.

8  
9           While the present invention has been described with reference to certain preferred  
10 embodiments, those skilled in the art will recognize that various modifications and other  
11 embodiments may be provided. For example, it may be desirable to configure the exam  
12 application for use on computers other than the user's personal computer. An institution may  
13 have a computer lab with computers used for many purposes. It is still desirable to prevent  
14 access to unauthorized files during an examination, but the exam application can be resident  
15 on the computers. More broadly, the invention can be used for any application where it is  
16 desirable to prevent access to unauthorized files while allowing the execution of a desired  
17 program. These other embodiments are intended to fall within the scope of the present  
18 invention, and these variations upon and modifications to the embodiments described herein  
19 are provided for by the present invention which is limited only by the following claims.

**CLAIMS**

What is claimed is:

1. A method for preventing access to unauthorized files stored in computer-readable media, the method comprising the steps of:
  - a) closing undesired processes running on the computer;
  - b) filtering user input to prevent access to unauthorized files; and
  - c) allowing filtered user input to a desired application.
2. The method of claim 1, further comprising the step of saving a file corresponding to the user input.
3. The method of claim 2, further comprising the step of providing a word processing module for the filtered user input.
4. The method of claim 1, wherein the step of filtering user input comprises intercepting messages corresponding to user input, determining whether the messages would lead to access of an unauthorized file and modifying those intercepted messages that would lead to access of an unauthorized file.
5. The method of claim 4, wherein the step of filtering further comprises cross-process subclassing.

6. The method of claim 5, wherein cross-process subclassing employs hooks.
7. A method for administering a secure examination on a computer, the method comprising the steps of:
  - a) providing removable computer-readable media on which an exam application is stored;
  - b) determining the validity of the removable media;
  - c) executing the exam application;
  - d) closing all nonessential processes running on the computer;
  - e) filtering user input to prevent access to unauthorized files;
  - f) recording the filtered user input to the exam application;
  - g) saving a copy of the filtered user input to the removable media.
8. The method of claim 7, further comprising the step of recording user input that, without filtering, would have accessed unauthorized files to an auxiliary information file.
9. The method of claim 8, further comprising the step of saving an encrypted copy of the auxiliary information file.
10. The method of claim 7, further comprising the step of requiring a subsequent execution of the exam application to be authorized by a proctor disk.



11. The method of claim 7, further comprising the step of periodically recording the number of keystrokes entered in a given time period.

12. A removable computer-readable storage device for preventing access to unauthorized files comprising:

- a) instructions to close all undesired processes running on the computer;
  - b) instructions to filter user input to prevent access to unauthorized files;
- and
- c) instructions to allow filtered user input to a desired application.

13. The device of claim 12, further comprising instructions to save a file corresponding to the user input.

14. The device of claim 13, further comprising a word processing module for the filtered user input.

15. The device of claim 12, wherein instructions to filter user input comprise instructions to intercept messages corresponding to user input, determine whether the messages would lead to access of an unauthorized file, and modify those intercepted messages that would lead to access of an unauthorized file.

16. The device of claim 15, wherein the instructions to filter further comprise cross-process subclassing.

17. The device of claim 16, wherein cross-process subclassing employs hooks.
18. An executable computer program for administering a secure examination on a computer, the program provided at least in part on removable computer-readable media, the program comprising:
- a) instructions to determine the validity of the removable computer-readable media;
  - b) instructions to execute the exam application;
  - c) instructions to close all nonessential processes running on the computer;
  - d) instructions to filter user input to prevent access to unauthorized files;
  - e) instructions to record the filtered user input to the exam application;
  - f) instructions to save a copy of the filtered user input to the removable computer-readable media.
19. The program of claim 18, further comprising instructions to record user input that, without filtering, would have accessed unauthorized files to an auxiliary information file.
20. The program of claim 19, further comprising instructions to save an encrypted copy of the auxiliary information file.
21. The program of claim 18, further comprising instructions to subsequently execute the exam application in a manner authorized by a proctor disk.

22. The program of claim 18, further comprising instructions to periodically record the number of keystrokes entered in a given time period.

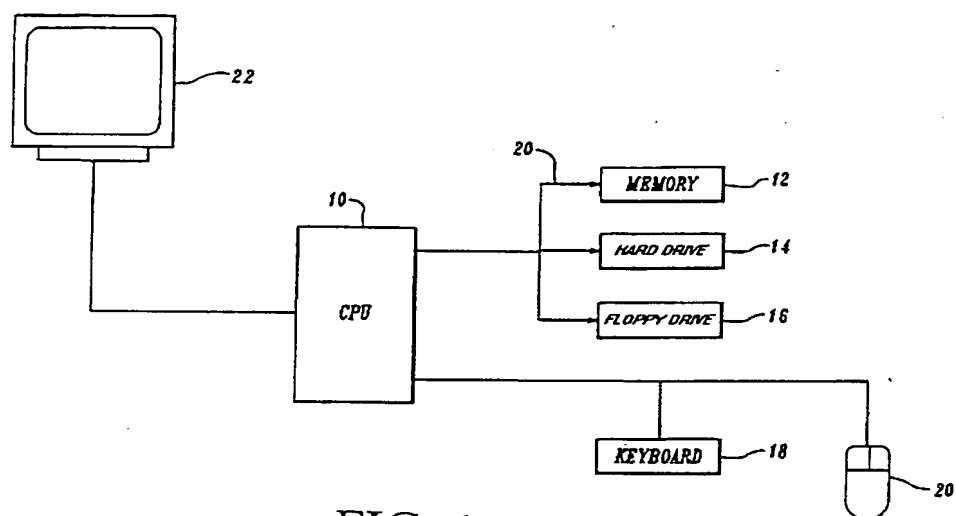
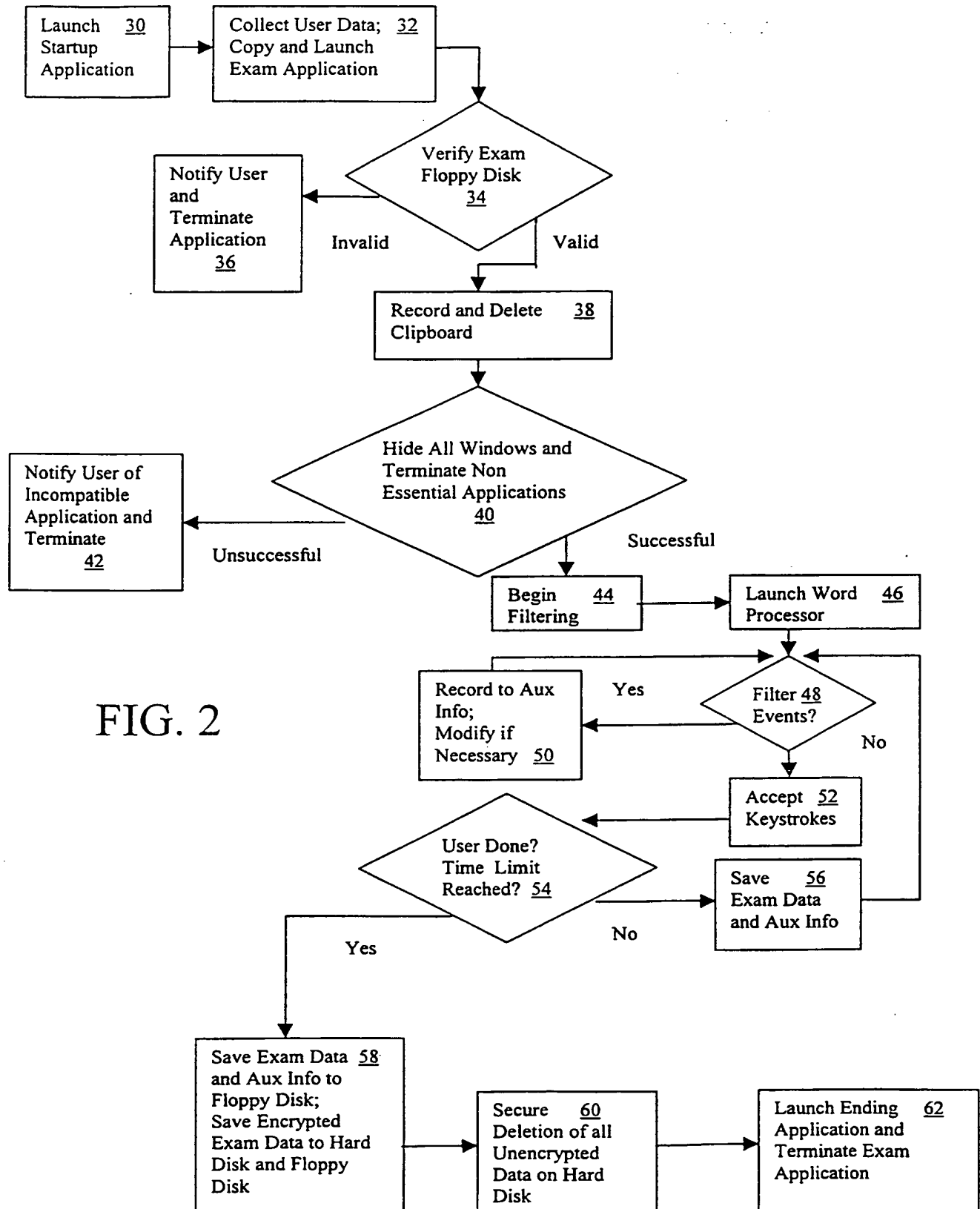


FIG. 1



# INTERNATIONAL SEARCH REPORT

International Application No

PCT/US 99/00481

## A. CLASSIFICATION OF SUBJECT MATTER

IPC 6 G06F1/00 G09B7/02

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 G06F G09B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 293 422 A (LOIACONO RONALD) 8 March 1994  see figures 1,2 see column 2, line 67 - column 6, line 6	1,2,4,5, 7,8,10, 12,13, 15,16, 18,19,21
A	WO 95 10095 A (EDUCATIONAL TESTING SERVICE) 13 April 1995 see figures 3,4,6,11-13 see page 8, line 5 - page 12, line 30 see page 16, line 9 - page 18, line 28	1,2,7, 12,13,18

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

### \* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

6 May 1999

Date of mailing of the international search report

14/05/1999

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

Weiss, P

# INTERNATIONAL SEARCH REPORT

information on patent family members

International Application No

PCT/US 99/00481

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5293422 A	08-03-1994	NONE	
WO 9510095 A	13-04-1995	CA 2149660 C	03-12-1996
		EP 0671039 A	13-09-1995
		JP 8504282 T	07-05-1996
		US 5513994 A	07-05-1996

**THIS PAGE BLANK (USPTO)**